

1 Thiago M. Coelho, SBN 324715  
2 *thiago@wilshirelawfirm.com*  
3 Shahin Rezvani, SBN 199614  
4 *srezvani@wilshirelawfirm.com*  
5 Jennifer M. Leinbach, SBN 281404  
6 *jleinbach@wilshirelawfirm.com*  
7 Jesenia A. Martinez, SBN 316969  
8 *jesenia.martinez@wilshirelawfirm.com*  
9 Jesse S. Chen, SBN 336294  
10 *jchen@wilshirelawfirm.com*  
11 **WILSHIRE LAW FIRM, PLC**  
12 3055 Wilshire Blvd., 12<sup>th</sup> Floor  
13 Los Angeles, California 90010  
14 Telephone: (213) 381-9988  
15 Facsimile: (213) 381-9989

16 *Attorneys for Plaintiff*  
17 *and Proposed Class*

18 **UNITED STATES DISTRICT COURT**  
19 **CENTRAL DISTRICT OF CALIFORNIA**

20 NICHOLAS BALSAMO, and DORLA  
21 STEWART, individually and on behalf of  
22 all others similarly situated,

23 Plaintiffs,

24 v.

25 CAESARS ENTERTAINMENT, INC., a  
26 Delaware corporation,

27 Defendant.

Case No.:

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

1 Plaintiffs Nicholas Balsamo and Dorla Stewart (“Plaintiffs”), individually and on behalf  
 2 of all others similarly situated, bring this action against Defendant Caesars Entertainment, Inc.  
 3 (“Caesars” or “Defendant”) based upon personal knowledge as to themselves and their own acts,  
 4 and as to all other matters upon information and belief, based upon, *inter alia*, the investigations  
 5 of their attorneys.

## 6 NATURE OF THE ACTION

7 1. In or around September of 2023, Caesars had their internal data servers breached  
 8 by unauthorized third-party hackers, who stole the highly sensitive personal identifying  
 9 information (“PII”) of its loyalty program members—including, *inter alia*, their names, driver’s  
 10 license numbers and social security numbers.

11 2. Caesars is a hospitality and entertainment company that operates destination  
 12 resorts throughout the United States. Customers who utilize Caesars’ service or stay at its resorts  
 13 may join its “Caesars Rewards” loyalty program, which allows those customers to earn  
 14 complimentary hotel stays, dinners and casino credits, among other rewards, by spending money  
 15 at Caesars’ locations. Caesars Rewards is the largest loyalty program in the gaming industry, with  
 16 over 60 million members.<sup>1</sup> In order to join the Caesars Rewards loyalty program, consumers must  
 17 provide Caesars with their PII.

18 3. Under statute and regulation, Caesars had a duty to implement reasonable,  
 19 adequate industry-standard data security policies safeguards to protect its customers’ and/or  
 20 employees’ PII. In particular, the PII was maintained on Caesars’ computer network in a condition  
 21 vulnerable to cyberattacks of this type. On information and belief, the PII was kept unencrypted  
 22 by Caesars’ as, had proper encryption been implemented, the criminals would have exfiltrated  
 23 only unintelligible data. As a result, its customers’ and/or employees’ sensitive information was  
 24 accessed and misused by unauthorized third-party hackers.

25 4. The potential for improper disclosure of Plaintiffs’ and Class Members’ PII  
 26 through a cyberattack was a known and foreseeable risk to Caesars, and Caesars was on notice  
 27 \_\_\_\_\_

28 <sup>1</sup> <https://www.vegashowto.com/caesars-rewards> (last accessed October 12, 2023).

1 that failing to take steps necessary to secure the PII from those risks left that property in a  
2 dangerous condition.

3 5. In addition, Caesars and its employees failed to properly monitor the computer  
4 network and systems that housed the PII. Had Caesars properly monitored its computer property,  
5 it would have prevented the attack or otherwise discovered the intrusion sooner.

6 6. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter  
7 “Class Members”), bring this class action to secure redress against Caesars for its reckless and  
8 negligent violation of their privacy rights.

9 7. Plaintiffs and Class Members are current and former customers of Caesars and  
10 current and former members of the Caesars Rewards program, who had their PII collected, stored,  
11 and ultimately breached by Caesars.

12 8. Plaintiffs and Class Members have suffered injuries and damages as a result of  
13 Caesars’ misconduct. As a direct and proximate result of Caesars’ wrongful actions and inactions,  
14 Plaintiffs and Class Members’ PII—including, *inter alia*, their names, driver’s license numbers  
15 and Social Security numbers—was compromised in the Data Breach, in violation of their privacy  
16 rights. Plaintiffs and Class Members are now exposed to a present and continuing risk of identity  
17 theft and fraud for the remainder of their lifetimes and must spend time and money on  
18 prophylactic measures, such as increased monitoring of their personal and financial accounts and  
19 the purchase of credit monitoring services, to protect themselves from future loss. Further,  
20 Plaintiffs and Class Members have lost the value of their PII, which is property and has  
21 determinable market value on both legitimate and dark web marketplaces. Finally, Plaintiffs and  
22 Class Members lost the benefit of their bargain, as they would not have become members of the  
23 Caesars Rewards Programs and subsequently spent money for Caesars’ services had they known  
24 that Caesars would not implement reasonable and adequate safeguards to protect their PII.

25 9. Plaintiffs and Class Members seek to remedy these harms and prevent any future  
26 data compromise on behalf of themselves and all similarly situated persons whose personal data  
27 was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate  
28 data security.

1           10.     Plaintiffs and Class Members have a continuing interest in ensuring that their  
2 information, which remains in the possession of Defendant, is and remains safe, and they should  
3 be entitled to injunctive and other equitable relief in addition to damages.

#### 4                                   **THE PARTIES**

5           11.     Plaintiff Nicholas Balsamo is a citizen and resident of the State of California.  
6 Plaintiff Balsamo has been a Caesars Rewards member for at least the last fifteen years and has  
7 on several occasions booked hotel rooms at Defendant's locations and utilized Defendant's  
8 services at those locations. On or around October 10, 2023, Plaintiff Balsamo received a data  
9 breach notice from Defendant Caesars informing him that his PII—specifically his name and  
10 drivers' license or other government issued ID number—had been breached by unauthorized  
11 third-party hackers.

12           12.     Plaintiff Dorla Stewart is a citizen and resident of the State of Nevada. Plaintiff  
13 Stewart has been a Caesars Rewards member since approximately 2012 and has on several  
14 occasions booked hotel rooms at Defendant's locations and utilized Defendant's services at those  
15 locations. On or around October 10, 2023, Plaintiff Stewart received a data breach notice from  
16 Defendant Caesars informing her that her PII—specifically her name and drivers' license or other  
17 government issued ID number—had been breached by unauthorized third-party hackers.

18           13.     Defendant Caesars Entertainment, Inc. is a Delaware corporation with its principal  
19 place of business located at 100 West Liberty Street, 12th Floor, Reno, Nevada, 89501. Defendant  
20 owns and operates entertainment and hospitality establishments throughout the United States.  
21 Defendant's registered agent for service of process is the Corporation Service Company, who can  
22 be served at 2710 Gateway Oaks Drive, Suite 150N Sacramento, CA 95833-3505.

#### 23                                   **JURISDICTION AND VENUE**

24           14.     This Court has subject matter jurisdiction over the claims asserted herein pursuant  
25 to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There exist members of the putative  
26 Plaintiff class that are domiciled in states diverse from Defendant, including Plaintiff Balsamo.  
27 Further, there are more than 100 putative class members, many of whom reside outside of the  
28

1 state of Nevada and have different citizenship from Defendant,<sup>2</sup> and the amount in controversy  
2 exceeds \$5 million, exclusive of interest and costs.

3 15. The Court also has personal jurisdiction over the Parties because Defendant  
4 routinely conducts business in California<sup>3</sup> and has sufficient minimum contacts in California to  
5 have intentionally availed themselves to this jurisdiction.

6 16. Venue is proper in this District because, among other things: (a) Plaintiff Balsamo  
7 resides in this District and is a citizen of this State; and (b) Defendant directed its activities at  
8 residents in this District.

### 9 **FACTUAL ALLEGATIONS**

#### 10 **A. Defendant's Business and Data Privacy Representations**

11 17. Defendant Caesars is a hotel and casino entertainment company that offers dining,  
12 entertainment, accommodations, gaming, and shopping services at its locations across the United  
13 States. As a part of those services, Defendant offers a loyalty program, Caesars Rewards, to its  
14 customers. Though the Caesars Rewards program, customers can earn points by spending money  
15 at Caesars' locations and redeem them for various benefits.

16 18. To become a Caesars Rewards member, customers are required to provide Caesars  
17 with their PII—including, *inter alia*, their names and driver's license numbers and/or social  
18 security numbers. Defendant then collects, aggregates, and stores that PII in its internal data  
19 servers.

20 19. In connection with this collection of customer PII, Caesar made promises and  
21 representations to its customers, including Plaintiffs and Class Members, that the PII it collected  
22 from them would be kept private and protected from unauthorized third party access. These  
23 representations can be found in, *inter alia*, Caesars' customer-facing Privacy Policy.

---

24  
25 <sup>2</sup> For instance, that Defendant posted a Data Breach Notice to the Office of the California Attorney  
26 General, indicates that the total number of affected California residents, the vast majority of which  
27 are likely citizens of California, affected by the data breach exceed 500. *See*  
<https://oag.ca.gov/ecrime/databreach/reports/sb24-574969>.

28 <sup>3</sup> Caesars operate at least two hotels and casinos in the State of California.  
<https://www.caesars.com/destinations#California> (last accessed October 12, 2023).

20. Caesars' Privacy Policy states that "Caesars Entertainment, Inc. and its subsidiaries and affiliates...value you as a customer and are committed to respecting your data privacy."<sup>4</sup> It goes on to state, in a section titled "Security," that "[w]e maintain physical, electronic, and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."

21. Upon information and belief, Caesars presents this Privacy Policy to customers who sign up for the Caesars Rewards program in-person at its locations. Caesars also presents this Privacy Policy to customers who sign up for the Caesars Rewards program online.

22. Consumers who wish to join the Caesars rewards program may do so by visiting the Caesars.com website and clicking the "My Rewards" link on the top right of the page. Doing so will lead the consumer to the <https://www.caesars.com/myrewards> webpage. There, a consumer may then join the Caesars Rewards program by clicking on the "Benefits" button on the top left of the page and then clicking "Join Now," or by clicking "Sign In" on the top left of the page and then clicking "Join Now." Doing so will lead the consumer to the <https://www.caesars.com/program/> webpage, wherein a consumer can click "I have a Caesars Rewards Number" to activate an account they previously created, or the "Create a new account" button to create a new Caesars Rewards account. Clicking the latter will lead a consumer to the <https://www.caesars.com/a/security/register.aspx> webpage, where the consumer will be prompted to enter their PII to join the Caesars Rewards program.

23. Importantly, on that final webpage, a consumer is prompted to check a clickwrap agreement stating that "I agree to be bound by the Program Rules and Regulations and the Privacy Policy as they may be updated from time to time" in order to proceed with their registration. This clickwrap agreement includes a link to Caesars' Privacy Policy.

---

<sup>4</sup> Privacy Policy <https://www.caesars.com/corporate/privacy> (last accessed October 12, 2023).


**CAESARS  
REWARDS®**

**CREATE ACCOUNT**

First name  Last name

Country  State  Postal code


Date of Birth (MM/DD/YYYY)

 +1  Phone Number

Which Caesars Rewards Property are you signing up from?

Create your sign-in credentials.

Email address

Create a password   Show

☐ I agree to be bound by the Program Rules and Regulations and Privacy Policy as they may be updated from time to time.

**JOIN US**

24. Caesars also includes its Privacy Policy when customers book hotel rooms on its website. When a customer uses the Caesars website to book a hotel room at one of its properties, they are presented with the following representation, which includes a link to the above-described Privacy Policy.



25. Both Plaintiff Balsamo and Plaintiff Stewart have booked hotel rooms through Caesars' website and would thus have been exposed to this representation.

### **B. The Data Breach**

26. In or around September of 2023, Caesars' internal data systems were subjected to unauthorized access and exfiltration by The Scattered Spider, a hacking group. As a result of this attack, The Scattered Spider took approximately six terabytes of data from Caesar—which included Caesars Rewards program member PII, such as names, driver's license numbers and/or social security numbers.<sup>5</sup>

27. This data breach was the result of a cyber-attack expressly designed and targeted to gain access to private and confidential data—including (among other things) the personal information, or PII, of Defendant's customers and clients, including Plaintiff's and Class Members' and, possibly, employees' PII—known to be stored in Defendant's internal data servers.

28. According to Caesars' September 7, 2023 filing with the United States Securities and Exchange Commission, the attack was facilitated through a "social engineering attack on an outsourced IT support vendor used by Caesar."<sup>6</sup>

### **C. Caesars' Statutory Obligation to Protect Customers' & Employees' PII**

29. Under Nevada Revised Statute Section 603A.210, Caesars, as a Nevada-headquartered corporation that collects nonpublic personal information and records it, was required to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

30. Upon information and belief, Caesars failed to implement such reasonable security measures—including proper security vetting of its third-party IT vendors—to protect the sensitive

<sup>5</sup> <https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14/> (last accessed October 12, 2023).

<sup>6</sup> <https://www.sec.gov/ix?doc=/Archives/edgar/data/0001590895/000119312523235015/d537840d8k.htm> (last accessed October 12, 2023).



1 PII entrusted to it by its customers, and instead allowed it to be accessed, disclosed, and used by  
2 unauthorized third-party hackers, in violation of this statute.

3 31. Further, the Federal Trade Commission Act, 15 U.S.C. §45 prohibits Caesars from  
4 engaging in “unfair or deceptive acts or practices affecting commerce.”

5 32. The Federal Trade Commission has found The Federal Trade Commission has  
6 found that a company’s failure to maintain reasonable and appropriate data security for the  
7 consumers’ sensitive personal information is an “unfair practice” in violation of the Federal Trade  
8 Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir.  
9 2015).

10 33. Caesars failed to comply with each of these state and federal statutes by failing to  
11 implement and maintain reasonable security procedures to protect Plaintiffs and Class Members’  
12 PII.

13 **D. Applicable Standards of Care**

14 34. In addition to their obligations under state and federal law, Caesars owed a duty  
15 to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing,  
16 safeguarding, deleting, and protecting the PII in their possession from being compromised, lost,  
17 stolen, accessed, and misused by unauthorized persons.

18 35. Caesars owed a duty to Plaintiffs and the Class Members to provide reasonable  
19 security, including consistency with industry standards and requirements, and to ensure that their  
20 computer system and networks, and the personnel responsible for them, adequately protected the  
21 PII of Plaintiff and Class Members.

22 36. Caesars owed a duty to Plaintiffs and the Class Members to design, maintain, and  
23 test their computer system to ensure that the PII in Caesars’ possession was adequately secured  
24 and protected, particularly prior to providing to third-party agents such as IT vendors.

25 37. Caesars owed a duty to Plaintiffs and the Class Members to create and implement  
26 reasonable data security practices and procedures to protect the PII in their possession, including  
27 adequately training their employees, agents and vendors and others who accessed the PII in their  
28 possession on how to adequately protect PII.

1 38. Caesars owed a duty of care to Plaintiffs and Class Members to implement  
2 processes that would detect a breach of their data security systems in a timely manner.

3 39. Caesars owed a duty to Plaintiffs and the Class Members to act upon data security  
4 warnings and alerts in a timely fashion.

5 40. Caesars owed a duty to Plaintiffs and Class Members to disclose if their computer  
6 systems and data security practices, including the computer systems and data security practices  
7 of its third-party agents or vendors, were inadequate to safeguard individuals' PII from theft  
8 because such an inadequacy would be a material fact in the decision to provide or entrust their  
9 PII to Caesars.

10 41. Caesars owed a duty to Plaintiffs and the Class Members to disclose in a timely  
11 and accurate manner when the data breach occurred.

12 42. Caesars owed a duty of care to Plaintiffs and the Class Members because they  
13 were the foreseeable and probable victims of any inadequate data security practices. Caesars  
14 received PII from Plaintiffs and Class Members with the understanding that Plaintiffs and Class  
15 Members expected their PII to be protected from disclosure. Caesars knew that a breach of its  
16 data systems would cause Plaintiffs and Class Members to incur damages.

17 43. Caesars breached these duties of care by, *inter alia*, failing to maintain reasonable  
18 and adequate data security safeguards, failing to ensure the data security of its third-party agents  
19 and/or vendors, and failing to disclose to these deficiencies to Plaintiffs and Class Members.

20 44. Specifically, Caesars claims that the data breach resulted from a social engineering  
21 attack on one of its third-party IT vendors. Social engineering is a common, well-recognized and  
22 highly-preventable form of data attack wherein the attackers use human interaction—often by  
23 impersonating employees or repair personnel— to obtain or compromise information about an  
24 organization or its computer systems. There are many known ways to prevent or deter social  
25 engineering attacks, including the implementation of multi-factor authentication, external and  
26 internal web application scanning, utilizing web WAF, penetration testing, and identity  
27  
28

1 verification procedures.<sup>7</sup>

2 45. Despite social engineering attacks being a common and well-known avenue of  
3 customer data theft, and despite the variety of safeguards by which companies that handle  
4 customer data can prevent such attacks, Caesars failed to implement such safeguards and/or failed  
5 to ensure that the data vendors it provided customer PII to implement such safeguards. In doing  
6 so, Caesars violated its duties to Plaintiffs and Class Members.

7 **E. The Data Breach Was a Foreseeable Risk of Which Defendant Was**  
8 **On Notice**

9 46. Caesars' data security obligations were particularly important given the substantial  
10 increase in cyber-attacks and/or data breaches in the hospitality services industry preceding the  
11 date of the breach.

12 47. Data breaches, including those perpetrated against the hospitality services sector  
13 of the economy, have become widespread.

14 48. In fact, similar data breaches have occurred recently involving other Nevada based  
15 hotels/casinos, which should have put Caesars on notice of the threat of cyberattacks against  
16 casinos due to the sensitive PII that they maintain.<sup>8</sup>

17 49. According to Bluefin, "[t]he restaurant and hospitality industries have been hit  
18 particularly hard by data breaches, with hotel brands, restaurants and establishments targeted by  
19 hackers in 2019."<sup>9</sup>

20 50. Another report says that the "companies in the food and beverage industry are the  
21 most at risk from cybercriminals."<sup>10</sup>

---

22  
23  
24 <sup>7</sup> <https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/>  
(last accessed October 12, 2023).

25 <sup>8</sup> See, e.g., <https://www.databreaches.net/nevada-restaurant-services-inc-provides-notice-of-data-privacy-event/>;  
26 <https://www.jdsupra.com/legalnews/crystal-bay-casino-notifies-86-291-2253639/>. (last accessed on October 12, 2023)

27 <sup>9</sup> <https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-consumer-data/> (last accessed on October 12, 2023).

28 <sup>10</sup> <https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack> (last accessed on October 12, 2023).

1           51. According to Kroll, “data-breach notifications in the food and beverage industry  
2 shot up 1,300% in 2020.”<sup>11</sup>

3           52. In 2021, a record 1,862 data breaches occurred, resulting in approximately  
4 293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>12</sup>

5           53. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive  
6 records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive  
7 records (9,700,238) in 2020.<sup>13</sup>

8           54. Indeed, cyber-attacks, such as the one experienced by Caesars, have become so  
9 notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a  
10 warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore,  
11 the increase in such attacks, and attendant risk of future attacks, was widely known and  
12 completely foreseeable to the public and to anyone in Caesars’s industry, including Caesars.

#### 13           **F. The Value of PII**

14           55. It is well known, and the subject of many media reports, that PII is highly coveted  
15 and a frequent target of hackers. Especially in the technology industry, the issue of data security  
16 and threats thereto is well known. Despite well-publicized litigation and frequent public  
17 announcements of data breaches, Caesars opted to maintain an insufficient and inadequate system  
18 to protect the PII of Plaintiffs and Class Members.

19           56. Plaintiffs and Class Members value their PII because in today’s electronic-centric  
20 world, their PII is required for numerous activities, such as new registrations to websites, or  
21 opening a new bank account, as well as signing up for special deals or receiving preferred loan  
22 rates.

23           57. Legitimate organizations and criminal underground alike recognize the value of  
24 PII. That is why they aggressively seek and pay for it.

---

26 <sup>11</sup> [https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-](https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336)  
27 [other-industries/d/d-id/1341336](https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336) (last accessed on October 12, 2023).

28 <sup>12</sup> See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at <https://notified.idtheftcenter.org/s/>), at 6.

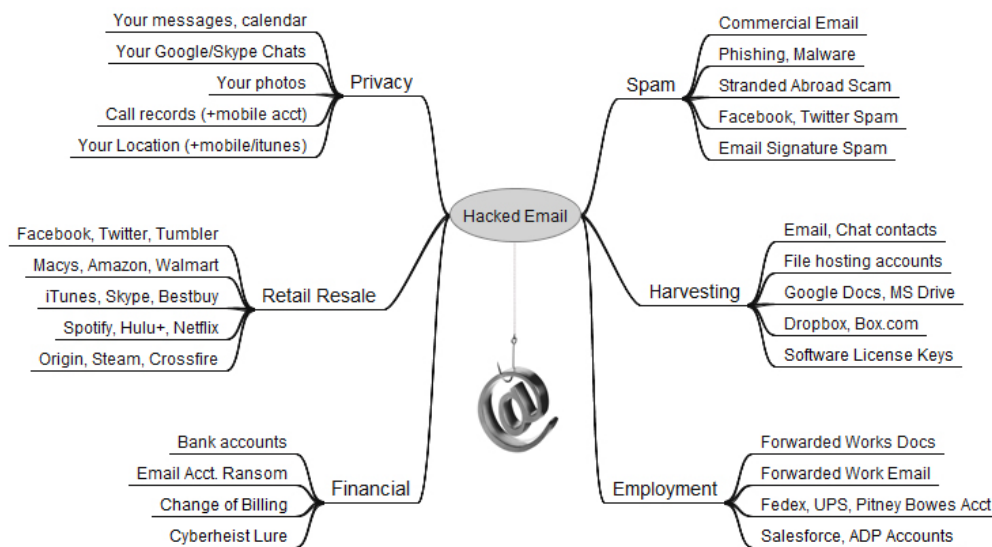
<sup>13</sup> *Id.*

58. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as “dumps.”<sup>14</sup>

59. Once someone buys PII, it is then used to gain access to different areas of the victim’s digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim’s accounts, as well as from those belonging to family, friends, and colleagues.

60. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.<sup>15</sup>

61. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.<sup>16</sup>



<sup>14</sup> See *All About Fraud: How Crooks Get the CVV*, Krebs on Security (April 26, 2016), <https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/>.

<sup>15</sup> *Identity Theft and the Value of Your Personal Data*, Trend Micro (Apr. 30, 2015), <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data>. (last accessed June 19, 2023).

<sup>16</sup> Brian Krebs, *The Value of a Hacked Email Account*, Krebs on Security (June 13, 2013, 3:14 PM), <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>. (last accessed June 19, 2023).

62. Hacked information can also enable thieves to obtain other personal information through “phishing.” According to the Report on Phishing available on the United States, Department of Justice’s website: “AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers.”<sup>17</sup>

63. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information, precisely as they have done here. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

64. Because a person’s identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

65. For example, armed with just a name and date of birth, a data thief can utilize a form of social engineering to obtain even more information about a victim’s identity, such as a person’s login credentials or Social Security number. This form of social engineering is a hacking technique whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

---

<sup>17</sup>*Report on Phishing* (Oct. 2006), [https://www.justice.gov/archive/opa/docs/report\\_on\\_phishing.pdf](https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf) (last accessed June 19, 2023).

66. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of “Fullz” packages.<sup>18</sup>

67. With “Fullz” packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

68. The development of “Fullz” packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

69. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

70. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

---

<sup>18</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/) (last accessed on October 13, 2023).



71. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

**G. Data Breach Victims Face a Heightened Risk of Identity Theft and Fraud**

72. Caesars failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiffs and the Class Members. The ramification of Caesars’ failure to keep Plaintiffs and the Class Members’ data secure is severe.

73. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice’s Bureau of Justice Statistics (“BJS”) found that “among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems.”<sup>19</sup> In fact, the BJS reported, “resolving the problems caused by identity theft [could] take more than a year for some victims.”<sup>20</sup>

**H. Annual Monetary Losses from Identity Theft are in the Billions of Dollars**

74. Javelin Strategy and Research reports that losses from identity theft reached \$21 billion in 2013.

75. Moreover, there may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

76. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO, Report to Congressional Requesters (June 2007), <http://www.gao.gov/new.items/d07737.pdf>. (last accessed June 19, 2023).

<sup>19</sup> See *Victims of Identity Theft*, U.S. Department of Justice (Dec 2013), <https://www.bjs.gov/content/pub/pdf/vit12.pdf>. (last accessed on October 13, 2023).

<sup>20</sup> *Id.*



77. This is particularly the case with data breaches such as Caesars, as the information compromised in this Data Breach, such as Social Security numbers, is immutable and cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft are one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.<sup>21</sup> Plaintiffs and the Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

#### **I. Plaintiffs and Class Members Suffered Damages**

78. The exposure of Plaintiffs' and Class Members' PII to unauthorized third-party hackers was a direct and proximate result of Caesars' failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law. The data breach was also a result of Caesars' failure to establish and implement appropriate administrative, technical, and physical safeguards—for both itself and for its third-party agents and vendors—to ensure the security and confidentiality of Plaintiffs' and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, as required by state and federal law.

79. Plaintiffs' and Class Members' PII is private and sensitive in nature and was inadequately protected by Caesars who was at all times fully aware of the potential for a cyberattack targeted at acquiring the PII collected and maintained by Caesars.

80. Caesars did not obtain Plaintiffs and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

81. As a direct and proximate result of Caesars' wrongful actions and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at a present, immediate,

---

<sup>21</sup> Michael Ollove, *The Rise of Medical Identity Theft in Healthcare* (Feb. 7, 2014), <https://khn.org/news/rise-of-identity-theft/>. (last accessed on October 13, 2023).

1 and continuing risk of harm from identity theft and identity fraud, requiring them to take the time  
2 and effort to mitigate the actual and potential impact of the subject data breach on their lives by,  
3 among other things, paying for credit and identity monitoring services, spending time on credit  
4 and identity monitoring, placing “freezes” and “alerts” with credit reporting agencies, contacting  
5 their personal, financial and healthcare institutions, closing or modifying personal, financial or  
6 healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts  
7 and healthcare accounts for unauthorized activity.

8 82. Plaintiffs have also lost the value of their PII. PII is a valuable commodity in both  
9 legitimate and dark web marketplaces, as evidenced by the \$200 billion valuation of the data  
10 brokering industry in 2019.<sup>22</sup> In fact, the data marketplace is so sophisticated that consumers can  
11 actually sell their non-public information directly to a data broker who in turn aggregates the  
12 information and provides it to marketers or app developers.<sup>23,24</sup> Numerous companies purchase  
13 PII directly from consumers, such as UBDI, which allows its users to link applications like  
14 Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave,  
15 which uses a similar business model. Consumers who agree to provide their web browsing history  
16 to the Nielsen Corporation can receive up to \$50.00 a year.<sup>25</sup>

17 83. And the value of PII is further demonstrated by market-based pricing data  
18 involving the sale of stolen PII across multiple different illicit websites.

19 84. Top10VPN, a secure network provider, has compiled pricing information for  
20 stolen PII, including \$160.15 for online banking details, \$35.00 for credit reports, and \$62.61 for  
21 passports. Standalone Yahoo email accounts have been listed for as little as \$0.41, while banking  
22 logins are in the range of \$500, and verified Paypal accounts with high balances are listed at as  
23 much as \$2,000.

---

24  
25 <sup>22</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>. (last accessed on  
October 13, 2023).

26 <sup>23</sup> <https://datacoup.com/>. (last accessed on October 13, 2023).

27 <sup>24</sup> <https://digi.me/what-is-digime/>. (last accessed on October 13, 2023).

28 <sup>25</sup> Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at  
<https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>. (last accessed on October 13,  
2023).

1           85. In addition, Privacy Affairs, a cyber security research firm, has listed the following  
2 prices for stolen PII:

- |   |   |       |
|---|---|-------|
| 3 | - U.S. driving license, high quality:           | \$550 |
| 4 | - Auto insurance card:                          | \$70  |
| 5 | - AAA emergency road service membership card:   | \$70  |
| 6 | - Wells Fargo bank statement:                   | \$25  |
| 7 | - Wells Fargo bank statement with transactions: | \$80  |
| 8 | - Rutgers State University student ID:          | \$70  |

9           86. Finally, Plaintiffs and Class Members have lost the benefit of their bargains with  
10 Caesars. Plaintiffs and Class Members would not have become members of Caesars Rewards and  
11 would not have spent money on Caesars' services—such as by booking hotel rooms and gaming  
12 at Caesars' locations—had they known that Caesars would not implement reasonable and  
13 adequate data security safeguards to protect their PII. As a result, Plaintiffs and Class Members  
14 have been injured and are entitled to damages at least equal to the difference in value between the  
15 price of the services they purchased from Caesars that include data security for their PII, and the  
16 services they actually received which did not.

17           87. Caesars' wrongful actions and inaction directly and proximately caused the theft  
18 and dissemination into the public domain of Plaintiffs and Class Members' PII, causing them to  
19 suffer, and continue to suffer, economic damages and other actual harm for which they are entitled  
20 to compensation, including:

- 21           a. The improper disclosure and theft of their PII;
- 22           b. The imminent and impending injury flowing from potential fraud and identity  
23           theft posed by their PII being exposed to and misused by unauthorized third-  
24           party hackers;
- 25           c. The untimely and inadequate notification of the data breach;
- 26           d. Ascertainable losses in the form of out-of-pocket expenses and the value of  
27           their time reasonably incurred to remedy or mitigate the effects of the data  
28           breach; and

- e. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market.
- f. Ascertainable losses in the form of Plaintiffs and Class Members' lost benefit of the bargain.

### CLASS ACTION ALLEGATIONS

88. Plaintiffs bring this action on their own behalf and pursuant to the Federal Rules of Civil Procedure Rules 23(a), (b)(2), (b)(3), and (c)(4). Plaintiffs intend to seek certification of a Nationwide Class, a California Subclass (represented by Plaintiff Balsamo), and a Nevada Subclass (represented by Plaintiff Stewart). The Classes are initially defined as follows:

The Nationwide Class, initially defined as:

All persons whose PII was compromised as a result of the cyber-attack that Defendant discovered on or around September 7, 2023, and who were sent notice of that data breach.

The California Sub-Class, initially defined as:

All persons residing in the State of California whose PII was compromised as a result of the cyber-attack that Defendant discovered on or around September 7, 2023, and who were sent notice of that data breach.

The Nevada Sub-Class, initially defined as:

All persons residing in the State of Nevada whose PII was compromised as a result of the cyber-attack that Defendant discovered on or around September 7, 2023, and who were sent notice of that data breach.

89. Excluded from each of the above Classes is Defendant, including any entity in which Caesars has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded or otherwise modified.

90. *Numerosity*, Federal Rules of Civil Procedure Rule 23(a)(1): The members of the Classes are so numerous that the joinder of all members is impractical. The disposition of the

1 claims of Class Members in a single action will provide substantial benefits to all parties and to  
 2 the Court. The Class Members are readily identifiable from information and records in  
 3 Defendant's possession, custody, or control, such as reservation receipts and confirmations.

4 91. *Commonality*, Federal Rules of Civil Procedure Rules 23(a)(2) and (b)(3): There  
 5 are questions of law and fact common to the Classes, which predominate over any questions  
 6 affecting only individual Class Members. These common questions of law and fact include,  
 7 without limitation:

- 8 a. Whether Defendant took reasonable steps and measures to safeguard  
 9 Plaintiffs' and Class Members' PII;
- 10 b. Whether Defendant violated common and statutory by failing to implement  
 11 reasonable security procedures and practices;
- 12 c. Whether Defendant took reasonable steps and measures to ensure Plaintiffs'  
 13 and Class Members' were safeguarded when provided to third-party agents or  
 14 vendors;
- 15 d. Whether Defendant violated common and statutory by failing to ensure its  
 16 third-party agents and vendors who were provided with customer PII  
 17 implemented reasonable security procedures and practices;
- 18 e. Which security procedures and which data-breach notification procedure  
 19 should Defendant be required to implement as part of any injunctive relief  
 20 ordered by the Court;
- 21 f. Whether Defendant knew or should have known of the security breach prior  
 22 to the disclosure;
- 23 g. Whether Defendant has complied with any implied contractual obligation to  
 24 use reasonable security measures;
- 25 h. Whether Defendant acts and omissions described herein give rise to a claim of  
 26 negligence;
- 27 i. Whether Defendant knew or should have known of the security breach prior  
 28 to its disclosure;

- j. What security measures, if any, must be implemented by Defendant to comply with its duties under state and federal law;
- k. The nature of the relief, including equitable relief, to which Plaintiffs and the Class Members are entitled; and
- l. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, and/or injunctive relief.

92. *Typicality*. Federal Rules of Civil Procedure Rule 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs are members of Caesars Rewards and customers of Defendant who had their PII breached by Defendant.

93. *Adequacy of Representation*, Federal Rules of Civil Procedure Rule 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intends to prosecute this action vigorously. Plaintiffs' claims are typical of the claims of other members of the Classes and Plaintiffs have the same non-conflicting interests as the other Class Members. Therefore, the interests of the Classes will be fairly and adequately represented by Plaintiffs and their counsel.

94. *Superiority of Class Action*, Federal Rules of Civil Procedure Rule 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

95. Damages for any individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied.

96. Class certification is also appropriate under Federal Rules of Civil Procedure Rules 23(a) and (b)(2), because Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is

appropriate as to the Classes as a whole.

## CAUSES OF ACTION

### FIRST CAUSE OF ACTION

#### Negligence

#### (On Behalf of Plaintiffs and the Nationwide Class)

97. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 96, inclusive, of this Complaint as if set forth fully herein.

98. In 2016, the Federal Trade Commission (“FTC”) updated its publication, “Protecting Personal Information: A Guide for Business,” which establishes guidelines for fundamental data security principles and practices for business.<sup>26</sup> Among other things, the guidelines dictate businesses should protect any personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses implement an intrusion detection system to expose breaches as soon as they occur; monitor all incoming traffic for activity indicating someone is attempting to infiltrate or hack the system; monitor instances when large amounts of data are transmitted to or from the system; and have a response plan ready in the event of a breach.<sup>27</sup> Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.<sup>28</sup>

99. Defendant owed Plaintiffs and the Class Members a duty of care in the handling of customers’ PII. This duty included, but was not limited to, keeping that PII secure and

---

<sup>26</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personalinformation.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf). (last accessed October 12, 2023).

<sup>27</sup> *Id.*

<sup>28</sup> Federal Trade Commission, *Start With Security: A Guide for Business* (Jun. 2015) <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>. (last accessed October 12, 2023).



1 preventing disclosure of the PII to any unauthorized third parties. This duty of care existed  
 2 independently of Defendants’ contractual duties to Plaintiffs and the Class Members. This duty  
 3 existed as to any third-party agents or vendors that Defendant provided customer PIII to. Under  
 4 the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Defendant is  
 5 obligated to incorporate adequate measures to safeguard and protect PII that is entrusted to them  
 6 in their ordinary course of business and transactions with customers.

7 100. Pursuant to Nevada Revised Statute Section 603A.210, Defendant, as a  
 8 corporation that collects nonpublic personal information and records it, was required to  
 9 “implement and maintain reasonable security measures to protect those records from  
 10 unauthorized access, acquisition, destruction, use, modification or disclosure.”

11 101. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a  
 12 duty to provide fair and adequate computer systems and data security practices to safeguard  
 13 Plaintiffs and Class Members’ PII. The FTC has brought enforcement actions against businesses  
 14 for failing to adequately and reasonably protect customer information, treating the businesses’  
 15 failure to employ reasonable and appropriate measures to protect against unauthorized access to  
 16 confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal  
 17 Trade Commission Act, 15 U.S.C. § 45. Orders from these actions further clarify the measures  
 18 businesses are required to undertake in order to satisfy their data security obligations.<sup>29</sup>

19 102. Additional industry guidelines which provide a standard of care can be found in  
 20 the National Institute of Standards and Technology’s (“NIST’s”) *Framework for Improving*  
 21 *Critical Infrastructure Cybersecurity* (Apr. 16, 2018), [https://nvlpubs.nist.gov/nistpubs/CSWP/](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)  
 22 [NIST.CSWP.04162018.pdf](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf). Among other guideposts, the NIST’s framework identifies seven  
 23 steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

24 Step 1: Prioritize and Scope. The organization identifies its  
 25 business/mission objectives and high-level organizational priorities. With this  
 26 information, the organization makes strategic decisions regarding cybersecurity

27 <sup>29</sup> Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*,  
 28 [https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-](https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement)  
[securityenforcement](https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-securityenforcement) ((last accessed June 19, 2023).



implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.

Step 2: Orient. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

Step 3: Create a Current Profile. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.

Step 4: Conduct a Risk Assessment. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific,

work best for their needs.

103. In addition to their obligations under federal regulations and industry standards, Defendant owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

104. Defendant owed a duty to Plaintiffs and the Class Members to design, maintain, and test their internal data systems to ensure that the PII in Defendant's possession was adequately secured and protected.

105. Defendant owed a duty to Plaintiffs and the Class Members to create and implement reasonable data security practices and procedures to protect the PII in its custodianship, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

106. Defendant owed a duty to Plaintiffs and the Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely manner.

107. Defendant owed a duty to Plaintiffs and the Class Members to act upon data security warnings and alerts in a timely fashion.

108. Defendant owed a duty to Plaintiffs and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material consideration in Plaintiffs and Class Members' decisions to entrust their PII to Defendant.

109. Defendant owed a duty to Plaintiffs and the Class Members to disclose in a timely and accurate manner when data breaches occur.

110. Defendant owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. Defendant collected PII from Plaintiffs and the Class Members. Defendant knew that a breach of its data systems would cause Plaintiffs and the Class Members to incur damages.

111. Defendant breached its duties of care to safeguard and protect the PII which Plaintiffs and the Class Members entrusted to it. Defendant adopted inadequate safeguards to protect the PII and failed to adopt industry-wide standards set forth above in its supposed protection of the PII. Defendant failed to design, maintain, and test its computer system to ensure that the PII was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

112. Defendant breached the duties set forth in 15 U.S.C. §45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs and Class Member's PII. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Defendant, *inter alia*, failed to adopt sufficient resources to identity and address security gaps.

113. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

114. As a direct and proximate result of Defendant's failure to adequately protect and safeguard the PII, Plaintiffs and the Class members suffered damages. Plaintiffs and the Class Members were damaged because their PII was accessed by third parties, resulting in increased

1 risk of identity theft, property theft and extortion for which Plaintiffs and the Class members were  
 2 forced to adopt preventive and remedial efforts. These damages were magnified by the passage  
 3 of time because Defendant failed to notify Plaintiffs and Class Members of the data breach until  
 4 weeks had passed. In addition, Plaintiffs and Class Members were also damaged in that they must  
 5 now spend copious amounts of time combing through their records in order to ensure that they  
 6 do not become the victims of fraud and/or identity theft.

7 115. Plaintiffs and Class Members have suffered actual injury and are entitled to  
 8 damages in an amount to be proven at trial but in excess of the minimum jurisdictional  
 9 requirement of this Court.

## 10 **SECOND CAUSE OF ACTION**

### 11 **Quasi-Contract/Unjust Enrichment**

#### 12 **(On Behalf of Plaintiffs and the Nationwide Class)**

13 116. Plaintiffs repeat and incorporate herein by reference each and every allegation  
 14 contained in paragraphs 1 through 115, inclusive, of this Complaint as if set forth fully herein.

15 117. Plaintiffs and Class Members provided their PII and conferred a monetary benefit  
 16 upon Defendant in exchange for services and/or employment. Plaintiffs and Class Members did  
 17 so under the reasonable but mistaken belief that part of their monetary payment to Defendant, or  
 18 the revenue Defendant derived from the provision of labor or use of the PII, would cover the  
 19 implementation of reasonable, adequate, and statutorily mandated safeguards to protect their PII.  
 20 Defendant was enriched when it diverted money intended to fund adequate data security towards  
 21 its own profit at the expense of Plaintiffs and Class Members.

22 118. Defendant's enrichment came at the expense of Plaintiffs and Class Members,  
 23 who would not have used Defendant's services, would not have provided their PII, or would not  
 24 have worked for Defendant, had they been aware that Defendant had not implemented reasonable,  
 25 adequate, and statutorily mandated safeguards to protect their PII.

26 119. Defendant enriched itself by saving the costs they reasonably should have  
 27 expended on data security measures to secure Plaintiffs' and Class Members' PII and instead  
 28 directing those funds to their own profits. Instead of providing a reasonable level of security that

1 would have prevented the hacking incident, Defendant calculated to increase its own profits at  
2 the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures.  
3 Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of  
4 Defendant's decision to prioritize its own profits over the requisite security.

5 120. Defendant knew that Plaintiffs and Class Members conferred a benefit which  
6 Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and  
7 Class Members for business purposes.

8 121. Defendant knew that the manner in which it maintained and transmitted PII  
9 violated industry standards and its fundamental duties to Plaintiffs and absent Class Members by  
10 neglecting well accepted security measures to ensure confidential information was not accessible  
11 to unauthorized access. Defendant had knowledge of methods for designing safeguards against  
12 unauthorized access and eliminating the threat of exploit, but it did not use such methods.

13 122. Defendant had within its exclusive knowledge, and never disclosed, that it had  
14 failed to safeguard and protect Plaintiffs and absent Class Members' PII. This information was  
15 not available to Plaintiffs, absent Class Members, or the public at large.

16 123. Defendant also knew that Plaintiffs and Class Members expected security against  
17 known risks and that they were required to adhere to state and federal standards for the protection  
18 of confidential personally identifying, financial, and other personal information.

19 124. Defendant should not be permitted to retain Plaintiffs' and Class Members' lost  
20 benefits, without having adequately implemented the data privacy and security procedures for  
21 itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal,  
22 state, and local laws. and industry standards. Defendant should not be allowed to benefit at the  
23 expense of consumers who trust Defendant to protect the PII that they are required to provide to  
24 Defendant in order to receive Defendant's services.

25 125. Plaintiff and Class Members have no adequate remedy at law.

26 126. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class  
27 Members have suffered injury and are entitled to damages in an amount to be proven at trial but  
28 in excess of the minimum jurisdictional requirement of this Court.

**THIRD CAUSE OF ACTION****Breach of Implied Contract****(On Behalf of Plaintiffs and the Nationwide Class)**

127. Plaintiffs repeat and incorporate by reference each and every allegation contained in paragraphs 1 through 127 inclusive of this Complaint as if set forth fully herein.

128. Defendant solicited and invited Plaintiffs and Class members to provide their PII to Defendant as a requirement of using its services, to become a member of Caesars' Rewards, or to be eligible for employment with Defendant. Plaintiffs and Class Members accepted those offers by providing their sensitive PII to Defendant in order to obtain those benefits and services from Defendant. In doing so, Plaintiffs and Class Members entered into implied contracts with Defendant.

129. Inherent within those implied contracts was a contractual obligation that Defendants would implement reasonable and adequate data security safeguards to protect the PII that Plaintiffs and Class Members entrusted to Defendant. Upon information and belief, Defendant makes representations to those who provide it with their PII that it will implement reasonable and adequate data security safeguards to protect their PII at the time they provide their PII to Defendant. These representations serve both as a basis for and as an acknowledgement by Defendant of these implied contractual duties.

130. Plaintiffs and Class Members provided their PII to Defendant under the reasonable but mistaken belief that Defendants would implement reasonable and adequate data security safeguards to protect that PII. However, Defendant did not provide such reasonable and adequate data security. Instead, Defendant allowed Plaintiffs' and Class Members' PII to be disclosed to unauthorized third-party hackers.

131. Defendant did not comply with federal statute and regulation and did not comply with industry data security standards. In doing so, Defendant materially breached their obligations under their implied contracts with Plaintiffs and Class Members.

132. That Defendant would implement reasonable and adequate data security to protect PII was a material prerequisite to Plaintiffs' and Class Members' provision of that PII to

Defendant. Plaintiffs and Class Members value the privacy of their PII, and do not disclose their PII to entities that do not protect it from unauthorized disclosure. Plaintiffs and Class members would not have provided their PII to Defendant had they known that Defendant would not implement such reasonable and adequate data security.

133. As a result of Defendant's breach, Plaintiffs and Class Members have been damaged. Plaintiffs and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiffs and the Class members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Defendant failed to notify Plaintiffs and Class Members of the data breach until weeks had passed. In addition, Plaintiffs and Class Members were also damaged in that they must now spend copious amounts of time combing through their records in order to ensure that they do not become the victims of fraud and/or identity theft.

134. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

#### **FOURTH CAUSE OF ACTION**

##### **Breach of Fiduciary Duty**

##### **(On Behalf of Plaintiffs and the Nationwide Class)**

135. Plaintiffs repeat and incorporate by reference each and every allegation contained in paragraphs 1 through 134 inclusive of this Complaint as if set forth fully herein.

136. Plaintiffs and Class Members provided their PII to Defendant in confidence and under the reasonable but mistaken belief that Defendant would protect the confidentiality of that information. Plaintiffs and Class Members would not have provided Defendant with their PII had they known that Defendant would not take reasonable and adequate steps to protect it.

137. Defendant's acceptance and storage of Plaintiffs' and Class Members' PII created a fiduciary relationship between Defendant and Plaintiffs and Class Members. As a fiduciary of Plaintiffs and Class Members, Defendant has duty to act primarily for the benefit of its patients and health plan participants, which includes implementing reasonable, adequate, and statutorily



1 complaint safeguards to protect Plaintiffs' and Class Members' PII.

2 138. Plaintiff and Class Members relied on the skill and expertise of Defendant to  
3 maintain the information entrusted to it as confidential. Defendant was in an exclusive position  
4 to guard against the foreseeable threat of a cyberattack and Plaintiff and Class Members had no  
5 way to verify the integrity of Defendant's data security or to influence its policies.

6 139. Defendant breached its fiduciary duties to Plaintiffs and Class Members by, *inter*  
7 *alia*, failing to implement reasonable and adequate data security protections, failing to comply  
8 with the data security guidelines set forth by the FTC, NIST and HIPAA, failing to implement  
9 reasonable and adequate data security training for its employees, and otherwise failing to  
10 reasonably and adequately safeguard the PII of Plaintiffs and Class Members.

11 140. As a direct and proximate result of Defendant's breaches of its fiduciary duties,  
12 Plaintiffs and Class Members have suffered damages. Plaintiffs and the Class Members were  
13 damaged because their PII was accessed by third parties, resulting in increased risk of identity  
14 theft, property theft and extortion for which Plaintiffs and the Class Members were forced to  
15 adopt preventive and remedial efforts. These damages were magnified by the passage of time  
16 because Defendant failed to notify Plaintiffs and Class Members of the data breach until weeks  
17 had passed. In addition, Plaintiffs and Class Members were also damaged in that they must now  
18 spend copious amounts of time combing through their records in order to ensure that they do not  
19 become the victims of fraud and/or identity theft.

20 141. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiffs and  
21 Class Members have suffered injury and are entitled to damages in an amount to be proven at  
22 trial but in excess of the minimum jurisdictional requirement of this Court.

### 23 **FIFTH CAUSE OF ACTION**

#### 24 **Violation of the Nevada Deceptive Trade Practices Act ("NDTPA")**

25 **Nev. Rev. Stat. Ann. §§598.0903, *et seq.***

26 **(On behalf of Plaintiff Stewart and  
the Nevada Sub-Class)**

27 142. Plaintiff Dorla Stewart ("Plaintiff for the purposes of this Count) repeat and  
28 incorporate by reference each and every allegation contained in paragraphs 1 through 141



1 inclusive of this Complaint as if set forth fully herein.

2 143. Plaintiff brings this Count on their own behalf and that of the Nevada Sub-Class  
3 (the “Class” for the purposes of this Count).

4 144. Defendant failed to “implement and maintain reasonable security measures” to  
5 protect Plaintiffs’ and Class Members’ sensitive PII, as required of it under Nev. Rev. Stat.  
6 §603A.210. Defendant’s failure to implement and maintain such reasonable security measures is  
7 evidenced by the fact that they allowed Plaintiff’s and Class Members’ sensitive PII to be  
8 accessed and exfiltrated by unauthorized third-party hackers.

9 145. Defendant’s violation of Nevada Revised Statute Section 603A.210 constitutes a  
10 deceptive trade practice under the NDTA. Nev. Rev. Stat. §603A.260.

11 146. Further, Defendant failed to provide Plaintiff and Class Members notification of  
12 the data breach in the most expedient time possible and without unreasonable delay, in violation  
13 of §603A.220. Despite learning of the data breach in November of 2022, and specifically learning  
14 that files had been copied from its data servers on November 27, 2022, Defendant delayed  
15 notifying Plaintiff and Class Members of the data breach until on or around February 24, 2022—  
16 approximately eighty-nine days later. Defendant has provided no reason or justification for this  
17 delay.

18 147. Defendant’s violation of Nevada Revised Statute Section 603A.220 further  
19 constitutes a deceptive trade practice under the Nevada Deceptive Trade Practices Act, Nevada  
20 Revised Statute Sections 598.0903, *et seq.* Nev. Rev. Stat. §603A.260.

21 148. Defendant’s violations were material to consumers, such as Plaintiff and Class  
22 Members. Had Plaintiff and Class Members known that Defendant would not implement  
23 reasonable and adequate data security safeguards to protect their PII, and that Defendant would  
24 not notify them of a data breach that had occurred within an expedient and timely manner, they  
25 would not have purchased Defendants’ services, or would have paid substantially less for them.

26 149. As a direct and proximate result of Defendant’s deceptive trade practices,  
27 Plaintiffs and Nevada Sub-Class members have suffered and will continue to suffer injury,  
28 including, *inter alia*, the loss of value of their PII, lost time and money spent dealing with the

1 fallout of the data breach, and the lost benefit of their bargain. Plaintiffs and Nevada Sub-Class  
 2 Members seek all monetary and non-monetary relief allowed by law, including damages, punitive  
 3 damages, and attorney's fees and costs.

4 **SIXTH CAUSE OF ACTION**

5 **Violation of the California Unfair Competition Law ("UCL")**  
 6 **Cal. Bus. & Prof. Code § 17200, *et seq.***  
 7 **(On behalf of Plaintiff Balsamo and the California Sub-Class)**

8 150. Plaintiff Nicholas Balsamo ("Plaintiff" for the purposes of this Count) repeats and  
 9 incorporates by reference each and every allegation contained in paragraphs 1 through 149  
 10 inclusive of this Complaint as if set forth fully herein.

11 151. Plaintiff brings this Count on his own behalf and that of the California Sub-Class  
 12 (the "Class" for the purposes of this Count).

13 152. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair  
 14 business practices within the meaning of California's Unfair Competition Law ("UCL"),  
 15 Business and Professions Code Sections 17200, *et seq.*

16 153. Defendant stored the PII of Plaintiff and Class Members in its computer systems.

17 154. Defendant knew or should have known that it did not employ reasonable, industry  
 18 standard, and appropriate security measures that complied with federal regulations and that would  
 19 have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that PII.  
 20 This included Defendant's failure to properly vet the data security of its third party agents and  
 21 vendors to whom it provided sensitive customer PII.

22 155. Defendant did not disclose at any time that Plaintiff's and Class Members' PII was  
 23 vulnerable to hackers because Defendant's data security measures were inadequate and outdated,  
 24 and Defendant was the only one in possession of that material information, which Defendant had  
 25 a duty to disclose.

26 156. Defendant's actions and inactions violated the "unlawful" prong of the UCL. As  
 27 noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation  
 28 for this UCL claim) by misrepresenting, by omission, the safety of their computer systems,  
 specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

157. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, by failing to ensure its affiliates with which it directly or indirectly shared the PII did the same, and by failing to timely notify Plaintiff and Class Members of the Data Breach.

158. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

159. Defendant's actions and inactions further violated the "unfair" prong of the UCL.

160. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged below.

161. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

162. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' PII

1 to third parties without their consent, diminution in value of their PII.

2 163. These unfair acts and practices were immoral, unethical, oppressive,  
3 unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members.  
4 They were likely to deceive the public into believing their PII was securely stored when it was  
5 not. The harm these practices caused to Plaintiffs and Class Members outweighed their utility, if  
6 any. Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively  
7 declared public policy, and is immoral, unethical, oppressive, and unscrupulous.

8 164. The harms suffered by Plaintiff and Class Members continues, as Plaintiff's and  
9 Class Members' PII remains in Defendant's possession, without adequate protection, and is also  
10 in the hands of those who obtained it without their consent.

11 165. Defendant's actions and omissions violated Section 5(a) of the Federal Trade  
12 Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[  
13 ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by  
14 consumers themselves and not outweighed by countervailing benefits to consumers or to  
15 competition"); *see also, e.g.*, In re LabMD, Inc., FTC Docket No. 9357, FTC File No. 102-3099  
16 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal  
17 information collected violated § 5(a) of FTC Act).

18 166. Plaintiff and Class Members suffered injury in fact and lost money or property as  
19 a result of Defendant's violations of the UCL. Plaintiffs and the California Class suffered from  
20 entering into transactions with Defendant that should have included adequate data security for  
21 their PII, by experiencing a diminution of value in their Private Information as a result if its theft  
22 by cybercriminals, the loss of Plaintiff's and Class Members' legally protected interest in the  
23 confidentiality and privacy of their PII, the right to control that information, and additional losses  
24 as described above.

25 167. As a result of Defendant's unlawful and unfair business practices in violation of  
26 the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable  
27 attorneys' fees and costs.  
28

**SEVENTH CAUSE OF ACTION****Violation of the California Consumer Privacy Act (“CCPA”)****Cal. Civ. Code § 1798.100, *et seq.*****(On behalf of Plaintiff Balsamo and the California Sub-Class)**

168. Plaintiff Nicholas Balsamo (“Plaintiff” for the purposes of this Count) repeats and incorporates by reference each and every allegation contained in paragraphs 1 through 167 inclusive of this Complaint as if set forth fully herein.

169. Plaintiff brings this Count on his own behalf and that of the California Sub-Class (the “Class” for the purposes of this Count).

170. Defendant violated Section 1798.150(a) of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information provided to it by Plaintiff and Class Members. This failure included Defendant’s failure to ensure that the customer PII it provided to its third-party agents and vendors was properly protected. As a direct and proximate result, Plaintiff and Class Members’ PII was subjected to unauthorized access and exfiltration, theft, or disclosure.

171. Defendant is an entity organized for the profit and/or financial benefit of its owners and, upon information and belief, buys, receives, sells, and/or shares, for commercial purposes, the PII of at least 50,000 individuals through, *inter alia*, its Caesars Rewards program.

172. As a direct and proximate result of Defendant’s actions and omissions alleged herein, Plaintiff and Class Members were injured and lost money, property, and/or the interest in the confidentiality and privacy of their PII, as well as additional losses as described above.

173. Plaintiff and Class Members have suffered actual injury and seek relief under §1798.150(a), including but not limited to, statutory damages no less than \$100 and up to \$750 per customer record subject to the data breach, recovery of actual damages; injunctive or declaratory relief requiring Defendant implement reasonable security policies and procedures to protect their PII that remains in its possession; any other relief the court deems proper; and attorneys’ fees and costs.

174. In compliance with Section 1798.150(b), Plaintiff Balsamo has sent a notice letter outlining Defendant’s specific violations of the CCPA to Defendant’s registered agent for service

1 of process contemporaneously with the filing of this Complaint. Plaintiff will seek to amend the  
 2 Complaint to seek relief once the requisite 30-day notice period has expired to state that Plaintiff  
 3 provided Defendant proper notice of this claim.

#### 4 **PRAYER FOR RELIEF**

5 WHEREFORE, Plaintiffs, individually and on behalf of all of the Class Members,  
 6 respectfully request that the Court enters judgment in their favor and against Defendant as  
 7 follows:

- 8 1. For an Order certifying the Classes as defined herein and appointing Plaintiffs and  
 9 their Counsel to represent the Classes;
- 10 2. For equitable relief enjoining Defendant from engaging in the wrongful conduct  
 11 complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and  
 12 Class Members' PII, and from refusing to issue prompt, complete, and accurate  
 13 disclosures to Plaintiffs and Class Members;
- 14 3. For equitable relief compelling Defendant to utilize appropriate methods and  
 15 policies with respect to consumer data collection, storage, and safety and to  
 16 disclose with specificity to Class Members the type of PII compromised;
- 17 4. For an award of actual damages, statutory damages, and compensatory damages,  
 18 in an amount to be determined at trial;
- 19 5. For an award of punitive and treble damages, in an amount to be determined at  
 20 trial;
- 21 6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable  
 22 by law; and
- 23 7. For such other and further relief as this Court may deem just and proper.

24 ///

25 ///

26 ///

27 ///

28 ///

**DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demands a jury trial for all claims so triable.

Dated: October 13, 2023

Respectfully Submitted,

/s/ Thiago M. Coelho

Thiago M. Coelho

**WILSHIRE LAW FIRM, PLC**

*Attorneys for Plaintiffs and Proposed Class*

**WILSHIRE LAW FIRM, PLC**  
3055 Wilshire Blvd, 12<sup>th</sup> Floor  
Los Angeles, CA 90010-1137